REMARKS

Claims 1-21 are pending. Claims 1-21 were rejected under 35 U.S.C. § 103. Claim 21 has been amended. Claims 22-24 have been added. Reconsideration and allowance of Claims 1-21, and allowance of Claims 22-24, is requested.

Rejection of Claims under 35 U.S.C. § 103

The Examiner rejected Claims 1-6, 9-14 and 17-21 under 35 U.S.C. § 103 as unpatentable over Chan et al. (U.S. Patent No. 6,005,942) in view of De Jong (U.S. Patent No. 5,802,519) and Le et al. (U.S. Patent No. 5,883,956).

Regarding Applicants' remarks in the Response to Office Action dated April 5, 2004 (referred to hereinafter as the "first Office Action response"), the instant Office Action states:

> Applicant argues the combination of Chan, de Jong and Le does not teach the described advantageous characteristics found in applicant's specification from page 10, line 10 to page 11, line 3 where the value of the access permission data (block 403) cannot be changed once that value is stored in the data storage device. Applicant further discusses an example where a single mass produced cryptographic device can be configured to meet either the robust cryptographic capabilities of domestic regulations or the less robust cryptographic capabilities of the export regulations. Examiner contends, Le teaches manufacturing a single secure processing unit (cryptographic device) for domestic use that can be reconfigured after manufacture for use in foreign countries (see column 2, lines 41-57). Once the secure processing unit is reconfigured for export use, the value for the access permissions are set and cannot be changed in order to meet the export restrictions. Therefore, the combination does meet the limitation of configuring the data storage device after manufacture such that the value for the access permissions is set for the specific cryptographic device. Accordingly, the examiner maintains the rejection given below.

As explained further below, the foregoing fails to respond to most of the remarks made in the first Office Action response regarding the patentability of the claims of this application in view of the bases for rejection of those claims given in the Office Action dated October 3, 2003 (referred to hereinafter as the "first Office Action"). Below, Applicants reiterate the remarks from the first Office Action response that have not been addressed in the instant Office Action and explain why the above characterization of the teaching of Le et al. is incorrect.

Claim 1 recites:

> A cryptographic device, comprising:
> means for performing one or more cryptographic operations; and
> a data storage device or devices for storing access permission data representing the availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein the data storage device or devices are adapted to enable all of the access permission data of the cryptographic device to be stored in the data storage device or devices after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed.

Regarding Claim 1, Applicants stated in the first Office Action response:

> As indicated above, the Examiner stated that "Chan fails to specifically teach storing access permission data in the ROM section of the smart card" and that "[n]either Chan nor De Jong specifically teach the access permission data represents the availability of one or more cryptographic characteristics." Thus, as understood by Applicants, the Examiner has acknowledged that neither Chan et al. nor De Jong teach storing all of the access permission data of a cryptographic device (i.e., data representing the availability of one or more cryptographic characteristics) in data storage

> device(s) of the cryptographic device such that once value(s) of the access permission data are stored in the data storage device(s), the value(s) of the access permission data cannot be changed. The Examiner further stated that "Le teaches a secure processing unit embodied in a PersonCard (smart card) which uses a capability table that defines the cryptographic functions a secure processing unit can perform" and that "[i]t would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications." However, the Examiner has not identified how Le et al. teach, alone or in combination with Chan et al. and/or De Jong, storing all of the access permission data of a cryptographic device in data storage device(s) of the cryptographic device such that once value(s) of the access permission data are stored in the data storage device(s), the value(s) of the access permission data cannot be changed. Thus, a prima facie case of unpatentability of Claim 1 has not been established.

Since the above remarks from the first Office Action response have not been addressed in the instant Office Action, Applicants request that the Examiner consider those remarks prior to issuing a further action in this application.

The instant Office Action states that Le et al. teach, at column 2, lines 41-57, "manufacturing a single secure processing unit (cryptographic device) for domestic use that can be reconfigured after manufacture for use in foreign countries" and that "[o]nce the secure processing unit is reconfigured for export use, the value for the access permissions are set and cannot be changed in order to meet the export restrictions." However, Le et al. do not teach at column 2, lines 41-57 that "[o]nce the secure processing unit is reconfigured for export use, the value for the access permissions are set and cannot be

changed in order to meet the export restrictions." Le et al. teach, at column 2, lines 41-57:

> Another need for an SPU which allows for customized configuration occurs in the manufacturing of integrated circuits for export to foreign countries. Due to export restrictions, only SPUs which do not support certain cryptographic operations, such as strong encryption, can be exported outside of North America. Therefore, unless an SPU design which supports reconfiguration is used, chip manufacturers would have to design and manufacture different SPUs depending upon whether it was intended for domestic uses or for export purposes. It is desirable to manufacture a single SPU designed for domestic use, but is also modifiable to satisfy export control requirements. This will reduce the production and inventory cost of SPUs significantly. In other words, it is desirable to design and build a single SPU and be able to modify its security features and functions to satisfy the security requirements of various applications.

The foregoing says nothing about whether the security features and functions of an SPU can or cannot be changed once established for export purposes and therefore does not support the contention in the Office Action that Le et al. teach that "[o]nce [a] secure processing unit is reconfigured for export use, the value for the access permissions are set and cannot be changed in order to meet the export restrictions." In fact, as already explained in the first Office Action response, Le et al. teach the opposite of such contention. Le et al. teach, at column 12, lines 10-23 (emphasis added):

> [A]fter [a] digital signature has been verified, [a] function extracts [an] "enabling bit string" from [an] external capability table and stores it in non-volatile RAM inside the SPU. If there exists a current capability table in the SPU's non-volatile RAM, the value of the new capability table would simply overwrite the value of the current capability table. ... The "enabling bit string" that is loaded in the SPU becomes the new capability table which governs the functions that an SPU can perform.

As the foregoing makes absolutely clear, Le et al. teach that a capability table stored in an SPU can be changed: the capability table (which defines the functions that the SPU can perform; see the Abstract of the Le et al. patent) is stored in a RAM (a data storage device in which stored data can be overwritten) and Le et al. explicitly state that "the value of [a] new capability table [can] simply overwrite the value of [a] current capability table." In fact, the ability to overwrite a capability table stored for use by an SPU is believed by Le et al. to constitute a significant advantage of their invention as compared to previous SPUs (see, e.g., column 3, lines 15-25 of the Le et al. patent). The teaching of Le et al. is so clear regarding the foregoing that, if the Examiner persists in contending that Le et al. teach that the configuration of a secure processing unit cannot be changed once a secure processing unit is configured for export use, the Examiner is requested to contact Applicants' undersigned attorney to discuss the matter further.

As previously indicated in the first Office Action response, in contrast, Claim 1 recites that "[a] data storage device or devices are adapted to enable all of the access permission data of [a] cryptographic device to be stored in the data storage device or devices after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the data storage device or devices, the value or values of the access permission data cannot be changed." Le et al. do not teach, either alone or in any combination with the teaching of Chan et al. or De Jong, a cryptographic device as

recited in Claim 1 and therefore do not provide the advantageous characteristics of such a cryptographic device. For example, as stated in Applicants' specification at page 10, line 10 to page 11, line 3 (emphasis added):

> Preferably, the access permission data of the cryptographic characteristic table 403 are stored in a programmable read-only memory (PROM). The use of such a data storage device enables flexibility in establishing the access permission data (i.e., the availability of cryptographic characteristics) of a cryptographic device, since the access permission data can be established at device fulfillment (see FIG. 1). Thus, a single mass-produced type of cryptographic device can be tailored to meet cryptographic needs for many different applications. Further, the use of such a data storage device enables permanency - and, therefore, security - in establishing the access permission data of a cryptographic device, since once the access permission data are established, the access permission data cannot be changed. Thus, a single mass-produced type of cryptographic device can be tailored to satisfy domestic demand for robust cryptographic capabilities or to conform to export regulations dictating somewhat less robust cryptographic capabilities, while, in the latter case, providing confidence that the limitations on the cryptographic capabilities cannot be circumvented once the cryptographic device has been exported to a user.

In particular, the invention taught by Le et al. does not provide permanency in establishing access permission data and therefore does not provide the security associated therewith. In view of the foregoing, Claim 1 is allowable over the combination of Chan et al., De Jong and Le et al.

Claims 2 and 3 each depend on Claim 1 and so are each allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 1.

Claim 4 recites:

> A computer readable storage medium or media of a cryptographic device, the computer readable storage medium or media encoded with instructions and/or data, comprising:
>
> instructions and/or data for performing one or more cryptographic operations; and
>
> access permission data stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more cryptographic operations are performed by the cryptographic device, wherein all of the access permission data is stored in a storage medium or media after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the storage medium or media, the value or values of the access permission data cannot be changed.

As discussed above with respect to Claim 1, Chan et al., De Jong and Le et al. do not teach, either alone or in any combination, a computer readable storage medium or media of a cryptographic device in which "access permission data is stored in a storage medium or media after manufacture of the cryptographic device such that once a value or values of the access permission data are stored in the storage medium or media, the value or values of the access permission data cannot be changed," as recited in Claim 4. Thus, Claim 4 is allowable over the combination of Chan et al., De Jong and Le et al.

Claims 5 and 18 each depend on Claim 4 and so are each allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 4.

Claim 6 recites:

> A cryptographic device, comprising:
> a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;
> one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and
> means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

The remarks made in the first Office Action response regarding the patentability of Claims 6, 9-14, 17 and 19-21 have not been addressed in any way in the instant Office Action. Those remarks are reiterated below. Applicants request that the Examiner consider those remarks prior to issuing a further action in this application.

In the first Office Action and in the instant Office Action, the Examiner stated that "[n]either Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device." The Examiner further stated in both the first Office Action and the instant Office Action that "Le teaches an external bus interface between [a] secure processing unit and a host system" and that "[t]his bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements

(column 7, lines 17-21)," then concluded that "[i]t would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications." Even assuming arguendo that the foregoing characterization of the teaching of Le et al. and its relationship to the teaching of Chan et al. and De Jong is true, such teaching is inapposite with respect to Claim 6, since Claim 6 recites "a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "allowing access to the first set of instructions and/or data from a device external to the cryptographic device." It has not been contended that Chan et al., De Jong or Le et al. teach or suggest a cryptographic device having such characteristics, alone or in any combination. Thus, a prima facie case of unpatentability of Claim 6 has not been established and Claim 6 is allowable over the combination of Chan et al., De Jong and Le et al.

A cryptographic device as in Claim 6 provides advantageous characteristics relative to previous cryptographic devices. For example, the first set of instructions and/or data recited in Claim 6 can be instructions and/or data for performing mathematical primitive operations (see, e.g., page 11, line 23 to

page 12, line 6 of Applicants' specification). As stated in Applicants' specification at page 12, lines 6-19:

> .... Exposing the mathematical primitive operations to the applications developer provides flexibility to the applications developer in creating application code.
>
> For example, to add a new cryptographic operation or modify an existing cryptographic operation, it is not necessary to download to the cryptographic device all of the code necessary to accomplish the cryptographic operation. Rather, since the mathematical primitive operations are already accessible on the cryptographic device 400, the applications developer can provide code at a higher (and simpler) level of abstraction that includes instructions, as necessary, to effect performance of the required mathematical primitive operations.

Claims 9-13 each depend on Claim 6, either directly or indirectly, and so are each allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 6.

Claim 14 recites:

> A computer readable storage medium or media encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:
>
> a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation;
>
> a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and
>
> a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part.

It has not been contended that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, a computer readable storage medium or media encoded with one or more computer programs including "a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part," as recited in Claim 14. Thus, a prima facie case of unpatentability of Claim 14 has not been established and Claim 14 is allowable over the combination of Chan et al., De Jong and Le et al.

Claim 17 depends on Claim 14 and so is allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 14.

Claim 19 depends on Claim 6 and so is allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 6.

Claim 20 depends on Claim 14 and so is allowable over the combination of Chan et al., De Jong and Le et al. for at least the reasons given above with respect to Claim 14.

As amended, Claim 21 recites:

> A cryptographic device, comprising:
>
> a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations;
>
> one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of

instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for enabling a third set of instructions and/or data that is distinct from both the first and second sets of instructions and/or data, that is used to perform one or more cryptographic operations, and that includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed to, after manufacture of the cryptographic device, be stored on the one or more data storage devices.

Regarding Claim 21, the Office Action states:

Chan teaches a smart card that includes an operating system capable of performing cryptographic operations (see column 4, lines 35-42 and column 7, lines 4-9). Chan further teaches the smart card contains three types of memory (data storage), one of which is persistent, non-mutable memory (ROM). At manufacture, the operating system and security related code are stored in the ROM section (see column 1, line 67 to column 2, line 11; column 7, lines 21-24 and column 13, lines 36-48). Chan fails to specifically teach storing sets of data (cryptographic operations and sub-operations of the cryptographic operations) in the ROM section for allowing access to a device external to the cryptographic device. De Jong's data structure is arranged to perform cryptographic operations in accordance with an external request for access and further performing a related sub-operation of the cryptographic operation (see column 15, lines 15-51). Neither Chan nor De Jong specifically teach allowing access to instructions and/or data from a device external to cryptographic device. Le teaches an external bus interface between the secure processing unit and a host system. This bus allows commands and data to be communicated to and from the secure processing unit and matches standard ISA bus requirements (see column 7, lines 17-21). It would have been obvious to one of ordinary skill in the art to combine the teachings of Le's system for configuring a secure processing unit and De Jong's coherent data structure for a smart card with Chan's system for a

> multi-application smart card for the purpose of designing and building a secure processing unit that can be reconfigured to satisfy the security requirements of various applications. By building only one type of secure processing unit, the production and inventory costs associated with manufacturing the secure processing unit can be reduced greatly [see Le et al; column 2, lines 41-57].

The foregoing remarks regarding Claim 21 duplicate the remarks made in both the first Office Action and the instant Office Action regarding Claim 6. However, the limitations of Claim 21 are not the same as those of Claim 6. Thus, it is clear that careful consideration has not been given to the patentability of Claim 21. In particular, there has been no contention that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, the limitations of the cryptographic device recited in Claim 21. For example, there has been no contention in the Office Action that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, "means for enabling a third set of instructions ... used to perform one or more cryptographic operations ... to, after manufacture of the cryptographic device, be stored on the one or more data storage devices," as recited in Claim 21. Thus, a prima facie case of unpatentability of Claim 21 has not been established and Claim 21 is allowable over the combination of Chan et al., De Jong and Le et al.

A cryptographic device as recited in Claim 21 can advantageously enable additional cryptographic capability to be added to a cryptographic device easily and efficiently. As

stated in Applicants' specification at page 12, lines 10-19 (and also discussed above):

> [T]o add a new cryptographic operation or modify an existing cryptographic operation, it is not necessary to download to the cryptographic device all of the code necessary to accomplish the cryptographic operation. Rather, since the mathematical primitive operations are already accessible on the cryptographic device 400, the applications developer can provide code at a higher (and simpler) level of abstraction that includes instructions, as necessary, to effect performance of the required mathematical primitive operations.

The Examiner rejected Claims 7, 8, 15 and 16 under 35 U.S.C. § 103 as unpatentable over Chan et al. (U.S. Patent No. 6,005,942) in view of De Jong (U.S. Patent No. 5,802,519), Le et al. (U.S. Patent No. 5,883,956) and Ehrsam et al. (U.S. Patent No. 3,962,539).

The remarks made in the first Office Action response regarding the patentability of Claims 7, 8, 15 and 16 have not been addressed in any way in the instant Office Action. Those remarks are reiterated below. Applicants request that the Examiner consider those remarks prior to issuing a further action in this application.

Claim 7 depends on Claim 6 and so includes the limitations of that claim. As discussed above, it has not been contended that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, a cryptographic device including "one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "means for allowing access to the first set of instructions and/or data from a device external to

the cryptographic device," as recited in Claim 6. Nor has it been contended that Ehrsam et al. teach or suggest, alone or in any combination with the teaching of Chan et al., De Jong or Le et al., a cryptographic device having such characteristics. Thus, a prima facie case of unpatentability of Claim 7 has not been established and Claim 7 is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al.

Claim 8 depends on Claim 7 and so is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al. for at least the reasons given above with respect to Claim 7.

Claim 15 depends on Claim 14 and so includes the limitations of that claim. As discussed above, it has not been contended that Chan et al., De Jong or Le et al. teach or suggest, alone or in any combination, a computer readable storage medium or media encoded with one or more computer programs including "a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation" and "a third set of instructions and/or data for allowing access to the first set of instructions and/or data from a device external to a cryptographic device of which the computer readable storage medium or media are part," as recited in Claim 14. Nor has it been contended that Ehrsam et al. teach or suggest, alone or in any combination with the teaching of Chan et al., De Jong or Le et al., a computer readable storage medium or media encoded with one or more computer programs including such instructions. Thus, a prima facie case of unpatentability of Claim 15 has not been

established and Claim 15 is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al.

Claim 16 depends on Claim 15 and so is allowable over the combination of Chan et al., De Jong, Le et al. and Ehrsam et al. for at least the reasons given above with respect to Claim 15.

In view of the foregoing, it is requested that the rejections of Claims 1–21 under 35 U.S.C. § 103 be withdrawn.

New Claims

Claims 22–24 have been added. Support for Claims 22 and 23 can be found in Applicants' specification at, for example, page 13, line 32 to page 14, line 26. Claims 22 and 23 each depend on Claim 21 and are therefore allowable as dependent on an allowable claim. Support for Claim 24 can be found in Applicants' specification at, for example, page 7, line 5 to page 9, line 13. Claim 22 depends on Claim 6 and is therefore allowable as dependent on an allowable claim.

CONCLUSION

Claims 1–21 were pending and were rejected. Claim 21 has been amended. Claims 22–24 have been added. In view of the

foregoing, it is requested that Claims 1-24 be allowed. If the Examiner wants to discuss any aspect of this application, the Examiner is invited to telephone Applicants' undersigned attorney at (408) 945-9912.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on December 14, 2004.

12-14-04 David R. Graham
Date Signature

Respectfully submitted,

David R. Graham

David R. Graham
Reg. No. 36,150
Attorney for Applicants